C9　マルウェア感染を判定する発見的手法について

発表者 0BDRM018 桑原 和也
指導教員 菊池 浩明 教授

Heuristics for Detecting Malware Attacks

Abstract: This paper studies the analysis on the CCC DataSet 2009 consisting of connection data observed by 94 decoy computers, called “honeypot”, for clarifying behavior of downloads of the malware and the port-scans. Based on the analysis, it is found that several malicious servers often coordinate to attack a single target hosts by sending some kinds of malware. The behavior, particularly observed in botnet, is defined as a *coordinated attack*. The paper proposes heuristic techniques for detection of the coordinated attack and reports the accuracy of the proposed heuristics. And also this paper analyzes the D3M 2010 Dataset, captured packets used in, Drive-by-Download attack, in order to investigate features on the communications and the trasmition of states. Based on the analysis of the observed behavior of all data, we propose a method for classification of attacks with sequence of path used by the attacks.

1　はじめに

インターネットが普及し利便性の高いサービスが提供される一方で，悪意のあるソフトウェアであるマルウェア (以下，MW) による被害が深刻化している．MWの攻撃手法は多様化・複雑化が進んでおり，感染時の振る舞いにも大きな変化がみられる．MWの攻撃手法には，数 100 万台の PC を従えたボットネットによる不正行為や Web サイト経由でのマルウェア感染による攻撃である Drive-by-Download 攻撃などが存在する．そこで，本研究ではボットネットに関する検知手法と Web 感染型マルウェアである Driveby-download 攻撃の検知手法を提案する．

2　データ解析

2.1　ボットネット

検出ルールを学習するデータとして，サイバークリーンセンター (以下，CCC) の 94 台のハニーポットで観測された通信データである CCC DATAset 2009 の攻撃通信データ [1] を用いる．1 台のハニーポットが起動して，(スケジュールに従って) リブートされるまでの観測期間を**スロット**という．攻撃通信データ 2 日分はスロットについて 145 個に分割される

全 145 のスロットの中で MW をダウンロードしているスロットは 58 件であった．これらを詳細に解析した結果，表 1 に示されるいくつかのルールを発見した．ルールは連携感染に関する Rule 1〜5，ポートスキャンに関する Rule 6〜8，MW に関する Rule 9〜10 がある．

2.2　Drive-by-Download 攻撃

NTT 情報流通プラットフォーム研究所の高対話型の Web クライアントハニーポットで収集した Web 感染型マルウェアの観測データである D3M 2010 の攻撃通信データ [1] を用いる．通常の通信から逸脱している通信の遷移を特定することにより，Drive-by-Download 攻撃固有のパスに注目し，次の 3 つの提案手法により攻撃の分類を試みる．

特徴量 A. Drive-by-Download 攻撃に用いられる通信の発信元 IP などの特徴.

特徴量 B. 一連の攻撃に用いられる URL のパス列.

特徴量 C. 攻撃に用いられる脆弱性の種類と数.

3　提案手法

3.1　連携感染パターンの発見的手法

2 章で述べた連携感染に関する規則に基づき，各ルールを並列に評価した合計スコアによる発見的手法を提案する．i 番目のスロットにおける Rule j の成立を $x_{ij} = 1$ と定める．スロット i のスコアは，$S_i = \sum_j^9 x_{ij}$ と定義する．このスコアが閾値以上かどうかで判定を行う．学習データにはあるハニーポットの 2 日間の全スロットデータを使用した．この学習データでは，連携感染しているスロットの最小スコアが 3 であった．そこで，閾値を 3 と定める．

精度 (ルールの成立割合) は，Rule 1 は 145 スロット中 17 スロットが該当しており (頻度)，その精度は `PE_VIRUT.AV` をダウンロードした全 38 スロット中，

Table 1: 連携感染の特徴を表わすルール一覧

NO.	ルール
Rule 1	PE_VIRUT.AV をダウンロードしたならば WORM_SWTYMLAI.CD と TROJ_BUZUS.AGB を同時刻にダウンロードを開始する.
Rule 2	WORM_SWTYMLAI.CD と TROJ_BUZUS.AGB のダウンロード直前に JOIN がある.
Rule 3	WORM_SWTYMLAI.CD と TROJ_BUZUS.AGB の DL サーバは常に一定.
Rule 4	PE_VIRUT.AV は 5 桁のポート番号使う.
Rule 5	WORM_SWTYMLAI.CD と TROJ_BUZUS.AGB はポート番号 80 番を使う
Rule 6	連携感染ならば，ポートスキャン先は PE_VIRUT.AV の DL サーバの第 1，2 オクテットと同じ.
Rule 7	IRC で“ JOIN ”を受信したならば約 5 秒後にポートスキャンを開始する.
Rule 8	連携感染したならば，1 秒間に 256 パケットのポートスキャンを連続して行う.
Rule 9	文字列“ MZ ”かつ“ PE ”を含むならば TCP による感染である.
Rule 10	UDP で win という文字列があれば，TFTP のダウンロードである.

WORM と TROJ をダウンロードしたものが 17 スロットあることを示している．145 スロット中 58 の感染スロットの中で連携感染を行っているスロットは 26 あり，約半分が連携感染である．

3.2 Drive-by-Download 攻撃の分類

提案した分類方法の有効性を既知の攻撃に対し評価を行う．既知の攻撃 G(ru:8080，インジェクション-3129 攻撃等) に対して，特徴量 A，特徴量 B，特徴量 C の 3 つの方式での識別した．既知攻撃 ru:8080 を識別する時の再現率，適合率は，

$$R_{A8080} = \frac{4}{13} = 0.31,$$
$$P_{A8080} = \frac{4}{49} = 0.08$$

であり，同様に 3126 に対しては，$R_{A3126} = 2/13 = 0.15$，$P_{A3126} = 2/5 = 0.4$ である以上により，A の総合的な精度をこれらの平均再現率で，

$$R_A = \frac{0.31 + 0.08}{2} = 0.20$$

と定める．再現率が低い理由は，A を定める際に，既知の攻撃を除外したためである．$G \times B$，$G \times C$ についても同様に $B4$ と $C1$，$C2$ を ru:8080 の識別条件として，再現率を求めると，$R_{B8080} = 2/13 = 0.15$, $R_{B3126} = 8/13 = 0.61$, $R_{C8080} = 4/13 = 0.31$, $R_{C3126} = 10/13 = 0.91$ であった．再現率の平均値は，

$$R_B = 0.38, R_C = 0.54$$

，従って，既知攻撃に対しては，C が最も精度が高い．

3.3 Drive-by-download 攻撃の検知に関する考察

3.2 節より既知攻撃に対して特徴量 C の精度が最も高かった．また，1 回の攻撃（1 つの URL の巡回）に対し，複数の脆弱性 が利用される傾向が確認された．これらの理由より，脆弱性の組み合わせを攻撃の検知に利用しようと考えた．解析結果として，3 つの攻撃パターンと複数の脆弱性パターンが存在した．

4 おわりに

CCC DATAset 2009 攻撃通信データにおける，感染種類を判定する発見的手法を報告した．評価データによる検出精度を明らかにした結果， 学習データに対して，2/28(7%) の誤検知 (FP) があったが，未検知 (FN) はなく，十分な精度が得られる手法である．一方，Drive-by-download 攻撃の分類に関しては，パスを用いた通信の振る舞いについて報告した．攻撃パターンにはそれぞれ特徴があり，多くの脆弱性が使われていた．従って，提案手法から攻撃パターンを正しく識別することは困難であった．脆弱性を用いた攻撃の検知に関しては，データ量が不十分であり，検知に有効であるとは言えない．今後の課題としては，クライアント型ハニーポットを作成し，長期間のデータを取得した上で，apriori や prefixspan のようなデータマイニングを用いる必要がある．

参考文献

[1] 畑田，他，“マルウェア対策のための研究用データセット ～ MWS 2010 Datasets ～”，マルウェア対策研究人材育成ワークショップ 2011（MWS2011），pp.1-8，2011.

業績リスト

1. K. Kazuya, et al., “Heuristic for Detecting Botnet Coordinated Attacks”, 4th International Workshop on Advances in Information Security (WAIS2010)，pp. 603-607，2010.
2. 桑原和也，他，“ボットネットの連携感染を判定する発見的手法について”，情報処理学会論文誌，Vol.51 No.9，pp. 1600-1609，2010.
3. 桑原和也，他，“パスシーケンスに基づく Drive-by-Download 攻撃の分類”，マルウェア対策研究人材育成ワークショップ 2010（MWS2010），pp. 771-776，2010.

他 1 件.